

BlackRock Client and Vendor Privacy Notice

Last revised: 18 December 2019

Introduction

BlackRock is committed to processing personal information ("PI"), including sensitive personal information ("SPI")¹, in line with all applicable privacy and data protection laws. Most of our offices are located in countries with laws governing the processing of PI. "BlackRock", "we", "us" or "our" means BlackRock, Inc., and each of the direct or indirect subsidiaries of BlackRock, Inc., (the "**BlackRock Group**"). BlackRock, Inc., BlackRock Group functions and the entity you contract with are the controllers of your PI. If your contract with the BlackRock Group is in connection with the investment in a BlackRock managed vehicle, the management company of the fund, together with the fund entity and, in circumstances where the investment manager is part of the BlackRock Group, that investment manager, will be the controller.

References to "you" or "your" refers to individuals whose PI is processed by BlackRock, including clients with direct or indirect relationships (such as those who invest through an intermediary); employees, contingent workers, officers, agents (together "**Representatives**"); and beneficial owners of an organization or entity in connection with:

- the provision of services to potential and actual clients;
- transactions to which we are party (including those which we effect on behalf of clients); or
- services provided to us by a third-party vendor.

This Privacy Notice sets out the purposes for which we collect, use and disclose (collectively "processing") PI and how it is protected. It also sets out individuals' rights in relation to the processing of their PI.

There may be additional terms, conditions and commitments that also govern how we collect, use and disclose your PI, which should be read in conjunction with this Privacy Notice.

Please click on the links below for further details:

- [PI we collect about you](#)
- [Purpose and legal basis for processing your PI](#)
- [To whom we disclose your PI](#)
- [International transfers and transfers to service providers](#)
- [Marketing and exercising your right to opt-out of marketing](#)
- [Third party marketing/sale of PI](#)
- [PI retention](#)
- [PI security](#)
- [Your rights](#)
- [Contacting us](#)
- [Complaints](#)
- [Cookie Notice](#)
- [Linked websites](#)
- [Changes to this Privacy Notice](#)

PI we collect about you

PI is information relating to an individual, which can be used either alone or with other sources of information to identify that individual. PI does not include information where the identity of the individual or the specific detail of the information has been removed and is therefore anonymous. SPI is a sub-category of PI that includes PI relating to race or ethnicity, religious or philosophical beliefs, sex life, sexual

¹ Please note not all privacy laws define SPI, for example Hong Kong, Singapore and Canada

orientation, political opinions, trade union membership, information about health and genetic and biometric data.

The nature of the information that we collect will depend on the services we provide and our relationship with you. We categorize PI we process as follows (the PI listed for each category are non-exhaustive examples):

- Identification data
Full name, title, gender, marital status, date of birth, passport number, driving licence number, national identification number, signature
- Contact data
Personal address, telephone number, email address
- Electronic Monitoring data
To the extent permitted by law, we may record and monitor your electronic communications with us
- Financial data
Bank account number; credit card number
- Marketing and Communications data
Marketing and communication preferences; tracking data relating to whether you have read marketing communications from us
- Professional Information data
Position/job title, work address; telephone number; email address
- Profile data
Username and password for our online services that you have access to; investments made by you; services requested; marketing communications responded to; survey responses
- Services data
Payment details to and from you; details of services you have provided to us or we have provided to you
- BlackRock Building and Assets Security data
Records of visits to our premises; CCTV recordings
- Technical data
Your use of and interaction with our online services; your IP address; browser type and version; browser plug in types and versions; operating system
- SPI
In limited circumstances, and where allowed by law, we may collect information about criminal convictions and offences, when legally required; dietary requirements if we are arranging catering, disability so that we can make reasonable accommodations for you in our buildings, sexual orientation if you provide details of your spouse or partner, political affiliations for us to determine whether you are a politically exposed person.

We collect PI in relation to you in a number of ways, including:

- when you provide it to us in connection with a BlackRock product or service, such as a completed investment application form
- if you are Representative of an organization or entity that is a client or vendor of BlackRock and that organization or entity provides us with your PI
- throughout the course of our relationship with you, including where you change your details, provide additional PI, or where the services we are providing to you change
- from public sources where you have manifestly chosen to make your PI public, including via public profiles on social media
- from third parties such as credit reference agencies
- from visits to our websites or through logging into any of our online services

We may also create or derive PI such as creating records of your interactions with us, subject to applicable law.

Unless we otherwise indicate that the provision of specific PI is optional, any PI we request is necessary for us to provide you or your organization or entity with the products and services requested. If you do not provide the PI requested, we may not be able to provide those products and services.

Purpose and legal basis for processing your PI

The below table sets out the purposes and basis for which we process PI.

Processing Purpose	Category of PI	Basis of Processing
To consider opening an account, or entering into a relationship at your request, including performing anti-money laundering, anti-terrorism, sanction screening, fraud and other due diligence checks	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Professional Information data • Services data • SPI 	<ul style="list-style-type: none"> • Performance of a contract • Legal or regulatory obligation • Legitimate interests: ensuring we do not accept the proceeds of criminal activities or assist in fraudulent or any unlawful activities, such as terrorism
To deliver the services you have requested, including liaising with third parties (i.e. brokers for the purposes of executing transactions) and to provide access to our technology solutions services (i.e. Aladdin)	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Profile data • Services data • Technical data • Marketing and Communications data • Professional Information data 	<ul style="list-style-type: none"> • Performance of a contract • Legal or regulatory obligation • Legitimate interests: ensuring that you are provided with the best client services and visitor services we can offer, and securing a prompt payment of any fees, costs and debts in respect of our services
To manage payments, fees and charges and to collect and recover money owed to us	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Professional Information data • Services data 	<ul style="list-style-type: none"> • Performance of a contract • Legitimate interests: ensuring we can manage payments, fees and charges and to collect and recover money owed to us
To manager our relationship with you which will include notifying you about changes to our terms of business or this privacy notice	<ul style="list-style-type: none"> • Identification data • Contact data • Profile data • Marketing and Communications data • Professional Information data 	<ul style="list-style-type: none"> • Performance of a contract • Legal or regulatory obligation • Legitimate interests: ensuring we can notify you about changes to our terms of business or this notice

To interact with governmental or regulatory bodies or other competent national authorities	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Services data • Professional Information data 	<ul style="list-style-type: none"> • Legal or regulatory obligation • Public interest
To detect or prevent fraud and/or other criminal activity and to protect our employees and assets	<ul style="list-style-type: none"> • Identification data • BlackRock Building and Assets Security data • Contact data • Electronic Monitoring data • Financial data • Professional Information data • Profile data • Services data • Technical data 	<ul style="list-style-type: none"> • Legal or regulatory obligation • Public interest • Legitimate interests: protecting BlackRock and client assets; detecting, and protecting against breaches of our policies and applicable laws; protecting BlackRock employees
To manage and protect our business, including improving data security, troubleshooting data and systems, system maintenance and testing, data hosting, managing our offices and other facilities	<ul style="list-style-type: none"> • Identification data • Contact data • Profile data • Technical data • Marketing and Communications data • Professional Information data 	<ul style="list-style-type: none"> • Legal or regulatory obligation • Legitimate interests: ensuring the efficient and secure running of our business, including through office and facilities administration, maintaining information technology services, network and data security and fraud prevention
To invite you to take part in market insight or other events, or client seminars or similar events, and to manage your participation in them	<ul style="list-style-type: none"> • Identification data • Contact data • Profile data • Technical data • Marketing and Communications data • Professional Information data 	<ul style="list-style-type: none"> • Legitimate interests: ensuring our client records are up-to-date; promoting our client services; receiving feedback; improving our services; identifying ways to expand our business
To send you marketing (including by paper and electronic channels) communications and service updates.	<ul style="list-style-type: none"> • Identification data • Contact data • Profile data • Technical data • Marketing and Communications data • Professional Information data 	<ul style="list-style-type: none"> • Legitimate interests: reviewing how clients use, and what they think of, our services; identifying ways to improve and expand our business

In relation to vendor services:

Purpose and/or activity	Type of data	Legal basis for processing
To engage you or the organization or entity you work for as a new supplier, including performing anti-money laundering, anti-terrorism, sanctions, fraud and other background checks	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Services data • Professional Information data 	<ul style="list-style-type: none"> • Performance of a contract • Legal or regulatory obligation • Legitimate interests: ensuring we do not deal with proceeds of criminal

		activities or assist in any other unlawful or fraudulent activities for example terrorism <ul style="list-style-type: none"> • Public interest
To manage payments, fees and charges and to collect and recover money owed to us	<ul style="list-style-type: none"> • Identification data • Contact data • Financial data • Professional Information data • Services data 	<ul style="list-style-type: none"> • Performance of a contract • Legitimate interests: ensuring we can manage payments, fees and charges; to collect and recover money owed to us
Where we provide you access to our systems we need to manage and protect our business, including improving data security, troubleshooting data and systems, system maintenance and testing, and data hosting	<ul style="list-style-type: none"> • Identification data • Contact data • Profile data • Technical data 	<ul style="list-style-type: none"> • Legal or regulatory obligation • Legitimate interests: ensuring the efficient and secure running of our business, including maintaining information technology services, network and data security

To whom we disclose your PI

In connection with one or more of the purposes outlined in the section 'Purpose and Legal basis for processing your PI' above, we may disclose PI in any jurisdiction to:

- other members of the BlackRock Group;
- professional advisors, third parties, agents or independent contractors that provide services to any member of the BlackRock Group (such as IT systems providers, platform providers, financial advisors, brokers, consultants (including lawyers and accountants));
- goods and services providers (such as providers of marketing services where we are permitted to disclose your personal information to them); intermediaries, brokers, and other individuals and entities that partner with us;
- competent authorities (including any national and/or international regulatory or enforcement body, agency, court or other form of tribunal or tax authority) or their agents where BlackRock is required or allowed to do so under applicable law or regulation;
- a potential buyer, transferee, merger partner or seller and their advisers in connection with an actual or potential transfer or merger of part or all of BlackRock's business or assets, or any associated rights or interests, or to acquire a business or enter into a merger with it;
- credit reference agencies or other organizations that help us to conduct anti-money laundering and anti-terrorist financing checks and to detect fraud and other potential criminal activity; or
- any person to whom disclosure is allowed or required by local or foreign law, regulation or any other applicable instrument.

International transfers and transfers to service providers

To provide global services and in the course of running our business, we may transfer PI to a location outside of the country where you reside or where services are provided to you or the organization or entity you work for, including BlackRock processing centers in the USA, Hungary, India and Singapore. Although the country to which PI may be transferred may not have the same level of privacy and data protection laws, we apply the same level of security and organizational controls to the processing of PI wherever it is processed. We require by contract that our third party service providers processing PI on our behalf to comply with BlackRock's criteria for PI processing.

If we transfer PI out of the EEA, we ensure a similar level of protection for your PI by ensuring the country is considered by the EU Commission to provide an adequate level of protection, putting in place contractual clauses the EU Commission consider to provide the same level of protection, or for third party service providers in the US, we may rely on the EU-US Privacy Shield certification.

Marketing and exercising your right to opt-out of marketing

We will not process your PI for marketing purposes if you have informed us you do not wish to receive marketing materials. You can request that we stop processing your PI for marketing purposes at any time by clicking on marketing opt-out links in any electronic marketing materials we send you, by making a request to your usual BlackRock contact or by using the contact details set out in the "Contacting Us" section of this Privacy Notice.

Third-party marketing/sale of PI

We do not share or sell your PI to third parties for the third party to use for their own marketing or other purposes.

PI retention

We will process your PI for as long as is necessary to fulfil the purpose for which it was collected or to comply with legal, regulatory, accounting, reporting, internal policy requirements or for the establishment or defense of legal claims.

PI security

We use a range of physical, electronic and managerial measures to ensure a level of security appropriate to the risk of PI processing. These measures include:

- education and training of relevant staff to ensure they are aware of our privacy obligations when processing PI as well as training around social engineering, phishing, spear phishing, and password risks;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

- the ability to restore the availability and access to PI in a timely manner in the event of a physical or technical incident;
- administrative and technical controls to restrict access to PI;
- technological security measures, including fire walls, encryption (industry standard SSL encryption with 128-bit key lengths), and anti-virus software;
- physical security measures, such building access controls;
- external technical assessments, security audits and vendor due diligence;
- perimeter security;
- segregation of networks;
- application security;
- endpoint security;
- Real-time monitoring of data leakage controls;
- Layered and comprehensive cybersecurity defences; and
- Security incident reporting and management.

The security of data transmitted over the internet (including by e-mail) cannot be guaranteed and carries the risk of access and interception. You should not send us any PI by open/unsecure channels over the internet. We endeavour to protect personal information but cannot guarantee the security of data transmitted to us or by us.

Your rights

In certain circumstances you may have the following rights in relation to the processing of your PI:

- **Access**
To request a copy of the PI we process in relation to you and to be informed about how we use and share your PI.
- **Object**
To object to the processing of your PI if (i) we are processing your PI on the grounds of legitimate interests or for the performance of a task in the public interest (including profiling); or (ii) if we are processing your PI for direct marketing purposes
- **Correction**
To request that we update the PI we process in relation to you, or to correct PI that you think is incorrect or incomplete.
- **Erasure**
To ask that we delete PI that we process in relation to you where we do not have a legal or regulatory obligation or other valid reason to continue to process it.

- **Restriction**

To request that we restrict the way in which we process your PI, for example, if you dispute the accuracy of your PI or have raised an objection which is under consideration.

- **Portability**

To request a copy of your PI that you have provided to us in a commonly used electronic format such as through the completion of an application form.

- **Automated decision making**

To request manual intervention if you are subject to automated decisions where the decision results in a legal or similar effect to you.

You may exercise your rights at any time by using the details set out in the Contacting us section. To the extent permitted by applicable law or regulation we reserve the right to charge an appropriate fee.

We may need to request specific information from you to help us confirm your identity and ensure your right to access to the PI requested, or to exercise any of your other rights. This is to ensure that PI is not disclosed to any person who does not have authority to receive it. We may also request further information in relation to your request to help us to locate the PI processed in relation to you, including, for example, the nature and location of your relationship with us.

We aim to respond to all legitimate requests within one calendar month. For example, if we think it may take us longer than one calendar month, (such as where your request is particularly complex or you have made a number of requests), we will notify you and keep you updated.

You will not be disadvantaged in any way by exercising your rights in relation to the processing of your PI.

Contacting us

The Global Head of Privacy and Data Protection oversees compliance with privacy and data protection at BlackRock. If you wish to exercise any of your rights, or have questions concerning this notice, please contact:

The Global Head of Privacy and Data Protection

BlackRock

12 Throgmorton Avenue

London

EC2N 2DL

Email: GroupPrivacy@BlackRock.com

If you are a California resident, you may also call us on +1 855 371 0019.

Complaints

If you have any concerns or complaints about the way your PI is processed, please contact the Global Head of Privacy and Data Protection at GroupPrivacy@BlackRock.com. You also have a right to complain to a data protection or other competent authority with jurisdiction over privacy and data protection law in the

country you live or work, or in the country where you believe an issue in relation to the processing of your PI has arisen. Please contact GroupPrivacy@BlackRock.com for further details.

Cookie Notice

Please see our separate Cookie Notice.

Linked websites

This Privacy Notice is not applicable to third party websites that we do not own or control, or to any third-party website where BlackRock advertisements are displayed.

Changes to this Privacy Notice

We may modify or amend this Privacy Notice from time to time and you are advised to visit our website regularly to check for any amendments. Any material changes will be communicated to you through an appropriate channel, depending on how we normally communicate with you.